WILLKIE FARR & GALLAGHER LLP

1875 K Street, N.W.
Washington, DC 20006-1238

Tel: 202 303 1000
Fax: 202 303 2000

July 6, 2026

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

On behalf of Redtail Technology, Inc. ("Redtail"), an information and technology solutions provider for financial services companies, located at 17605 Wright Street, Omaha, NE 68130, I am writing to notify your office of an incident that may have affected the security of certain personal information relating to one (1) New Hampshire resident. Redtail is providing this notice on behalf of certain business customers for which Redtail stores or maintains data, as identified below. By providing this notice, Redtail does not waive any rights or defenses regarding the applicability of New Hampshire Law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 13, 2026, Redtail experienced a social engineering attack against an employee by which an unauthorized third party gained temporary access to a limited subset of data and cloud platforms used by the Redtail team to manage and support our customer relationships. Once inside, the unauthorized actor exfiltrated data from these systems. Upon detecting the event, Redtail's security systems contained the threat quickly and prevented additional access by the unauthorized user. The unauthorized user was removed from Redtail's systems early in the day on May 14, 2026.

Redtail immediately worked with counsel and a leading third-party cybersecurity investigator to understand the nature and scope of the incident, including identifying any potentially implicated personal information.

Upon becoming aware of unauthorized access, Redtail began a review to determine the nature of the information that was potentially accessed, as well as the identity of individuals to whom the information relates. That process was recently completed, and identified that certain information related to Redtail business customers was potentially accessed by the unauthorized actor. In particular, the investigation identified information about one (1) New Hampshire resident that was potentially accessed, and this information includes the individual's name and Social Security Number.

Notice to Data Owners and New Hampshire Residents

On June 8, 2026, Redtail notified the affected business customer data owner about the potential involvement of personal information collected through them. Since then, Redtail has been working with the data owner to facilitate appropriate notifications to individuals and regulators. This notification is submitted as part of that process and on behalf of J.W. Cole Advisors, Inc. as the data owner.

On July 6, 2026, Redtail will mail written notice of this incident to the affected New Hampshire resident on behalf of the data owner. Among other things, the notification includes an offer of complimentary credit monitoring and identity theft protection services for 24 months through Experian. The letter also includes information and recommendations for affected individuals to protect themselves, including by remaining vigilant for signs of identity theft or fraud by reviewing account statements and monitoring their credit reports. A template copy of the notification letter is included with this letter.

Other Steps Taken To Address the Incident

Redtail has implemented additional security measures on the affected systems, such as by strengthening access controls, and providing additional alerts and training for employees to protect against similar occurrences in the future.

Contact Information

Should you have any questions regarding this event, please contact me at 202-303-1125.

Best,

Daniel K Alvarez

Daniel Alvarez

Enclosure: Sample Notification Letter

J.W. Cole Advisors, Inc.
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 6, 2026

Q1323-LVC-0000003 P001 T00001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF DATA BREACH

Dear Sample A. Sample,

In June 2026, we learned that one of our service providers had experienced a data security breach. We are writing today to notify you that your personal data was affected by this breach, and to provide information to assist you in mitigating potential risks. *We have no reason to believe that your personal data has been misused.*

We take this incident seriously and sincerely regret any inconvenience it may have caused.

WHAT HAPPENED?

On May 13, 2026, our service provider experienced a social engineering attack against an employee by which an unauthorized third party gained temporary access to a limited subset of data and cloud platforms our service provider uses to serve its clients – including us. Once inside, the unauthorized actor began exfiltrating data from these systems.

Upon detecting the event, our service provider's security systems contained the threat quickly. The threat actor was removed from our service provider's systems early in the day on May 14, 2026.

WHAT INFORMATION WAS INVOLVED?

The external investigation confirmed that your personal data was affected by this incident, including your social security number and account number(s). While we have no evidence to suggest that your personal data has been misused in any way, it is important that you take appropriate precautions to mitigate the use of this information for malicious purposes.

WHAT WE ARE DOING

Our service provider has worked with a leading third-party cybersecurity investigator to understand the nature and scope of the incident, and has implemented security measures on the affected systems and protect against similar occurrences in the future, such as by further strengthening access controls and providing additional alerts and training for employees. Law enforcement and appropriate regulatory authorities have been notified.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 24 months. To start using the service, please follow the steps below:

- Ensure that you enroll by September 30, 2026 by 6:59 pm CT (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/1Bcredit
- Provide your activation code: ABCDEFGHI
- Provide your information when prompted

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by September 30, 2026 at 833-745-1385 Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

WHAT YOU CAN DO

As a best practice, you should remain vigilant and carefully review your personal and work accounts for any suspicious activity. We also urge you to consider the following actions to protect your personal data:

- Activate the complimentary identity theft protection services by following the instructions in this letter.
- Promptly change your personal and enterprise passwords, and ensure that two-factor authentication is enabled, especially on financial accounts. If you detect any unauthorized activity on an account, you should change the password and security questions associated with the account.
- Monitor your credit information, initiate a fraud alert with all three credit bureaus, and consider placing a freeze on your credit reports.

FOR MORE INFORMATION

Please accept our apologies that this incident has occurred. We are committed to maintaining the privacy of personal information in our possession and that of our service providers**. If you have any further questions regarding this incident, please contact my office at** 603-262-3510 from 9:00 – 5:00 ET, Monday – Friday. You may also contact my Investment Advisors Compliance Department, J.W. Cole Advisors, Inc., at (813) 935-6776.

Sincerely,

Doug Wright, CRPC

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:
equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
866-349-5191

Experian:
experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:
transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

- **For Colorado, Delaware, and Illinois residents:** You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.
- **For Maryland residents:** You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023.
- **For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.
- **For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.
- **For Georgia, Maryland, New Jersey, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).
- **For New York residents:** You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, http://www.ag.ny.gov/home.html, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, http://www.dos.ny.gov/consumerprotection, 1-800-697-1220.